Adagium: Jurnal Ilmiah Hukum
E-ISSN: 2985-5128
Volume 4 Number 2 (2026), pp. 1681-1709
DOI: https://doi.org/10.70308/t09by734

Reconstructing Digital-Forensic Authentication of Electronic Evidence in AI-Era Criminal Proceedings

Abigail Dwi Pangestu[1*], Happy Sunaryanto[2], Kurniawan Tri Wibowo[3]
[1] Universitas Pelita Harapan, Indonesia
[2,3] Universitas Amikom Purwokerto, Indonesia
*Correspondence: kurniawan@amikompurwokerto.ac.id

Received: 30 August 2026	Accepted: 02 October 2026	Published: 31 October 2026

Abstrak

Perkembangan artificial intelligence (AI) meningkatkan risiko manipulasi bukti elektronik, sementara Pasal 235 Undang-Undang Nomor 20 Tahun 2025 tentang KUHAP belum mengatur secara terperinci mekanisme teknis autentikasinya. Penelitian ini bertujuan menganalisis kecukupan pengaturan autentikasi alat bukti elektronik dan merekonstruksi mekanisme yang menjamin reliabilitas pembuktian pidana di era AI. Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan. Bahan hukum dikumpulkan melalui studi kepustakaan dan dianalisis secara kualitatif-preskriptif. Pengaturan autentikasi belum memadai karena kewenangan hakim tidak diimbangi standar pemeriksaan teknis, dukungan ahli digital forensik, dan infrastruktur verifikasi yang terintegrasi. Penelitian menawarkan model forensically supported judicial authentication melalui Peraturan Mahkamah Agung (PERMA) dan Electronic Evidence Authentication System (EEAS). Model ini mengintegrasikan preservasi bukti, verifikasi hash, pemeriksaan metadata dan provenance, deteksi manipulasi AI, verifikasi ahli, serta penilaian yudisial. Reliabilitas pembuktian membutuhkan integrasi norma hukum, kompetensi teknis, dan dukungan kelembagaan. Kebaruan penelitian terletak pada rekonstruksi autentikasi berlapis yang menghubungkan kewenangan hakim dengan verifikasi digital forensik terstandar tanpa mengalihkan kewenangan pengambilan keputusan dari hakim.

Kata Kunci: autentikasi; bukti elektronik; digital forensik; artificial intelligence; KUHAP

Abstract

The development of artificial intelligence (AI) increases the risk of manipulating electronic evidence, while Article 235 of Law Number 20 of 2025 concerning the Criminal Procedure Code has not regulated in detail the technical mechanism for authentication. This research aims to analyze the adequacy of the authentication arrangement of electronic evidence and reconstruct the mechanism that ensures the reliability of criminal evidence in the AI era. The research uses normative legal methods with legislative, conceptual, and comparative approaches. Legal materials are collected through literature studies and analyzed qualitatively-prescriptively. Authentication arrangements are inadequate because the judge's authority is not balanced by technical examination standards, the support of digital forensic experts, and an integrated verification infrastructure. The research offers a forensically supported judicial authentication model through the Supreme Court Regulation

(PERMA) and the Electronic Evidence Authentication System (EEAS). This model integrates evidence preservation, hash verification, metadata and provenance checks, AI manipulation detection, expert verification, and judicial assessment. The reliability of proof requires the integration of legal norms, technical competence, and institutional support. The novelty of the research lies in the reconstruction of layered authentication that connects the authority of judges with standardized forensic digital verification without shifting decision-making authority from judges.

Keywords: *authentication; electronic evidence; digital forensics; artificial intelligence; Criminal Procedure Code.*

INTRODUCTION

Digital transformation has changed the character of evidence in the criminal justice system.[1] Facts that were previously conveyed through testimony, physical documents, or material objects are now increasingly represented through photographs, videos, voice recordings, electronic conversations, metadata, and digital documents, in line with the increasing position of electronic data generated by computers, mobile phones, cloud services, and social media as evidence in criminal and civil cases.[2] This change gained legitimacy through Law Number 20 of 2025 concerning the Criminal Procedure Code, which recognizes electronic evidence as evidence in Article 235 paragraph (1) of the Criminal Procedure Code. However, this recognition poses a new challenge, namely ensuring that the digital information submitted at trial truly represents the facts to be proved; This challenge is both juridical and technical because it concerns the authentication of electronic evidence which is a requirement for ensuring the integrity, reliability, and evidentiary value of digital data.[3]

Unlike conventional evidence, electronic evidence is vulnerable because digital data is easily duplicated, moved, altered, and deleted, making it potentially contaminated.[4] Photos can be altered using software or *generative artificial intelligence*, videos can be engineered through *deepfakes*, sounds can be imitated, and digital conversations can be faked, because increasingly realistic synthetic media are now able to manipulate evidence and mimic individual identities.[5] Therefore, the problem of proof is not enough to be solved by showing the existence of a file, but must also include checking the authenticity, source, integrity, formation process, and history of its ownership through a *chain of custody mechanism* that maintains the trust and security of digital evidence throughout its life cycle.[6]

---

[1] I. R. Begishev and A. V. Mayorov, "Digital Transformation of Criminal Justice: Theoretical Foundations and Legal Regulation Issues," *Legal Order History Theory Practice* 48, no. 1 (2026): 67–72, https://doi.org/10.47475/2311-696x-2026-48-1-67-72.

[2] Kislay Chauhan, "Digital Evidence and Emerging Technologies," *Indian Journal of Law* 4, no. 2 (2026): 17–22, https://doi.org/10.36676/ijl.v4.i2.188.

[3] N. T. M Chanh, "Authentication of Electronic Evidence Derived from Digital Transactions and Communications," Zenodo, 2025, https://doi.org/10.5281/zenodo.17926440.

[4] G. Pestana, W. Antunes, and J. Carvalho, "Digital Chain of Custody Operational Framework," 2023, 417–22, https://doi.org/10.1109/techdefense59795.2023.10380890.

[5] C Kerdvibulvech, "Big Data and AI-Driven Evidence Analysis: A Global Perspective on Citation Trends, Accessibility, and Future Research in Legal Applications," *Journal of Big Data* 11, no. 1 (2024), https://doi.org/10.1186/s40537-024-01046-w.

The development of AI increases the risk of false evidence being accepted as authentic evidence, as synthetic audiovisual content is increasingly difficult to distinguish from original recordings, threatening the integrity and sacredness of evidence in criminal cases.[7] On the other hand, the widespread public awareness of the ability to manipulate digital manipulation makes evidence that is actually authentic vulnerable to being refuted as *deepfake*, a phenomenon known as *wild's dividend*, so that trust in visual evidence decreases and there is a risk of denial and impunity.[8] Both risks can interfere with the reconstruction of facts and affect the determination of guilt or innocence of the accused.

Article 235 paragraph (3) of the Criminal Procedure Code specifies that evidence must be able to be proven to be authentic and obtained without violating the law. Paragraph (4) gives the authority to the judge to assess the authenticity and validity of the acquisition of evidence. Furthermore, paragraph (5) determines that evidence that is inauthentic and/or obtained unlawfully cannot be used and does not have evidentiary power. This provision places the judge as a gatekeeper in determining the feasibility of evidence, in line with the character of the Indonesian codification-based evidentiary system and places the judge as a seeker of material truth as well as a procedural filter of digital evidence. However, the Criminal Procedure Code has not explicitly regulated the technical standards, examination procedures, and expertise support mechanisms needed to reliably test the authenticity of digital evidence.[9]

This condition shows that there is a gap between legal *authority* and institutional capacity. Judges are authorized to assess authentication, but do not automatically have digital forensic expertise to identify AI-based manipulation; limited cyber literacy among judges, prosecutors, and investigators, as well as the unavailability of accredited digital forensic laboratories, have also widened the gap between technology and justice. [10] Electronic proof checks can require analysis of metadata, *hash values*, file structures, and source devices, as timestamp checks, source device identities, and cryptographic hash values serve as digital identity markers to validate the authentication of evidence.[11] In fact, manipulation detection

---

[6] S. G. Nath, K. Summers, J. Baek, and G. Ahn, "Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics," 2024, 11–20, https://doi.org/10.1109/tps-isa62245.2024.00012.

[7] S. P. Kothari and S. Tibrewala, "AI's Trojan Horse: The Deepfake Conundrum under the Criminal Justice System," *GLS KALP: Journal of Multidisciplinary Studies* 4, no. 3 (2024): 45–53, https://doi.org/10.69974/mtzxrc12.

[8] K. R Thuemler, "The Collapse of Visual Certainty: Implications for Privacy, Surveillance, and Societal Accountability," Zenodo. European Organization for Nuclear Research, 2025, https://doi.org/10.5281/zenodo.18024038.

[9] R. Hardyansah and R. Saputra, "Convergence and Divergence: Strategies for Proving Digital Evidence in Common Law and Indonesian Law Systems," *Journal of Sovereign Law* 9, no. 1 (2026): 74, https://doi.org/10.30659/jdh.v9i1.51432.

[10] S Bhattarai, "Bridging the Digital Divide: The Imperative for Cyber Expertise among Nepal's Justices/Judges, Litigators, and Investigators," *KDCBAR Law Journal* 1, no. 1 (2025): 223–38, https://doi.org/10.3126/kdcbar.v1i1.86735.

[11] N. Sharma, S. Minhas, K. Singh, V. Vipin, S. Hait, and L. S. Rathore, "EvidenceX: A Comprehensive Digital Forensics Tool for Evidence Extraction," *International Journal of Scientific Research in Computer Science Engineering and Information Technology* 11, no. 2 (2025): 3828–36, https://doi.org/10.32628/cseit25112859.

devices have limitations in the form of *overfitting* tendencies, high computational complexity, and limited generalization of different *deepfake* creation methods , so the results of the examination still require critical evaluation.[12]

Without a structured examination mechanism, there is an inequality between the complexity of technology and the ability of judicial institutions to verify evidence, as well as the persistent gap between the high-capacity legal system and the resource-constrained system, particularly in the areas of technological infrastructure, digital literacy, and procedural protection.[13] Digital manipulation can be difficult to recognize through ordinary visual or auditory observation, while judges must still determine the authenticity of evidence as a basis for decision-making. Variations in electronic evidence examination practices also demonstrate the importance of consistent procedures, including the use of forensic digital examinations when the authenticity and integrity of evidence are in question.

These weaknesses show that Article 235 of the Criminal Procedure Code has regulated the authority and legal consequences of authentication, but has not adequately explained how authentication should be carried out. Each type of electronic evidence has different characteristics, so photo examination is not always the same as video examination, voice recording, or electronic conversation. Evidence generated or modified by AI even requires examination methods that can differ from conventional digital evidence. Therefore, authentication norms need to be supported by appropriate technical standards in order to be applied effectively.

Authentication is also directly related to the principles *of due process of law* and the protection of fair *trials*, as audiovisual evidence manipulated or generated by AI directly touches the principles of presumption of innocence and due process.[14] The acceptance of false evidence can form a construction of a case that does not correspond to reality, while the rejection of authentic evidence can eliminate important information for the defendant's defense. Such errors can affect the assessment of the elements of the criminal act, the judge's belief, and the legitimacy of the verdict. Thus, authentication is not just an administrative procedure, but a mechanism to ensure that digital evidence has a basis of reliability that can be accounted for.

A number of studies on electronic evidence in Indonesia highlight the issue of authentication standards, the continuity of the *chain of custody*, and the difference in institutional capacity in the examination of digital evidence. The need for digital forensics and verification mechanisms is increasingly important, especially since the applicable regulations in Indonesia have not explicitly regulated *deepfake* technology, making it difficult to qualify the law, collect evidence, and effectively enforce the law.[15] This condition shows that there is a regulatory gap between the recognition of electronic evidence and the need to test its reliability in the AI era.

---

[12] M. M. El-Gayar, M. Abouhawwash, S. Askar, and S. Sweidan, "A novel approach for detecting deep fake videos using graph neural networks," *Journal of Big Data* 11, no. 1 (2024), https://doi.org/10.1186/s40537-024-00884-y.

[13] M. I. Khan and I. Ahmed, "A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime and Digital Evidence," *5, no.* 2 (2024): 1–29, https://doi.org/10.63125/96ex9767.

[14] Y. M. Apollo and K. Michael, "Beyond a Reasonable Doubt? Audiovisual Evidence, AI Manipulation, Deepfakes, and the Law," *IEEE Transactions on Technology and Society 5, no.* 2 (2024): 156–68, https://doi.org/10.1109/tts.2024.3427816.

However, placing digital forensics as a technical solution alone does not answer the issue of judges' authority based on Article 235 of the Criminal Procedure Code. Digital forensic experts should not replace judges in determining the legal value of evidence. On the other hand, judges should also not be forced to conduct technical examinations outside of their competence. Therefore, a mechanism is needed that integrates the judge's authority, expert opinion, examination methods, *chain of custody*, and reliability standards so that authentication decisions do not rely solely on discretion without technical verification.

The main problem in this study is no longer the recognition of electronic evidence as evidence, but the adequacy of authentication mechanisms to ensure its reliability. The more complex digital manipulation technology is, the more difficult it is for authentication to be carried out only through juridical assessment without the support of forensic examinations. Without improvement, the application of Article 235 paragraphs (3) to (5) of the Criminal Code risks stopping at formal authentication, without guaranteeing substantive authenticity related to the integrity and origin of digital materials.

Based on these problems, it is necessary to reconstruct the concept of authentication from *the judge-centered authentication* approach towards *forensically supported judicial authentication*. This model maintains the judge as the holder of authority to determine the feasibility and strength of proof, but supports his decision through standardized forensic digital examination, data integrity verification, *provenance* and *chain of custody examination*, and expert involvement if necessary. Thus, this study is directed to test the adequacy of authentication design in Article 235 of the Criminal Procedure Code and formulate a mechanism that integrates legal aspects with digital forensics to ensure the integrity of criminal evidence in the era of artificial intelligence.

Legal scope and governing framework

Law 20 of 2025 is Indonesia's Criminal Procedure Code (KUHAP), not the substantive Criminal Code (KUHP). Article 235(1)(f) expressly recognises electronic evidence; Article 235(3) requires that evidence be capable of authentication and have been obtained without violating the law; Article 235(4) allocates evaluation of authenticity and lawful acquisition to judges; and Article 235(5) governs the consequence of a judicial finding of non-authenticity or unlawful acquisition. The expression 'authentic and obtained unlawfully' is therefore incorrect.[16]

Authentication, lawful acquisition, integrity, relevance and probative weight must not be conflated. A matching cryptographic hash can demonstrate that a particular copy matches the bytes of a specified baseline, provided the baseline itself is reliable. It cannot independently show who created the file, whether the scene represented is genuine, or whether a deepfake detector is accurate. Those issues

[15] R. N. A. Tobing and Y. Yuli, "Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media," *Eduvest: Journal of Universal Studies* 6, no. 2 (2026): 1302–14, https://doi.org/10.59188/eduvest.v6i2.52738.

[16] Republic of Indonesia, Law No. 20 of 2025 concerning the Criminal Procedure Code (KUHAP), art. 235(1), (3)–(5), https://perpajakan.ddtc.co.id/id/sumber-hukum/peraturan-pusat/undang-undang-20-tahun-2025.

require provenance records, chain-of-custody evidence, forensic methods open to challenge and judicial evaluation.

RESEARCH METHOD

This study uses normative legal research methods with a statute approach, a conceptual approach, and a comparative approach. The legislative approach is used to analyze Article 235 of Law Number 20 of 2025 concerning the Criminal Procedure Code, while the conceptual approach is used to formulate an authentication mechanism for electronic evidence in the era of artificial intelligence. The comparative approach is carried out by examining practices in the United States, Singapore, the United Kingdom and Wales, as well as the ENFSI digital forensic guidelines as material to build an authentication model that is relevant to the Indonesian criminal justice system.

Legal materials were collected through literature studies of laws and regulations, books, scientific journal articles, and relevant official documents. The analysis was carried out qualitatively and prescriptively to identify weaknesses in the electronic evidence authentication arrangements and formulate reconstruction through PERMA, the support of digital forensic experts, and the development of the Electronic Evidence Authentication System (EEAS), while still placing the judge as the final decision-maker regarding authenticity and evidentiary strength.

RESULTS AND DISCUSSION

The Adequacy of Electronic Evidence Authentication Arrangements in Article 235 of the Criminal Procedure Code to Ensure the Reliability of Criminal Evidence in the Era *of Artificial Intelligence*

Article 235 of Law Number 20 of 2025 concerning the Criminal Procedure Code brings an important change in the construction of Indonesian criminal evidence by placing electronic evidence as one of the evidence that can be used in examination at trial. The change marks a shift from the paradigm of proof that relies on conventional objects and information to a proof system that accommodates digital reality.[17] Article 235 paragraph (3) explicitly requires that evidence must be provable and obtained in a non-unlawful manner. Article 235 paragraph (4) then gives the authority to the judge to assess the authenticity and legality of obtaining evidence, while paragraph (5) stipulates the consequence that evidence that is declared inauthentic and/or unlawfully obtained cannot be used and does not have evidentiary force. The structure, on the one hand, shows the awareness of the lawmakers of the importance of authentication; on the other hand, it shows the institutional problem that authentication authority is given to judges without being accompanied by a design of technical capacity that explicitly guarantees the judge's ability to carry it out.

This problem becomes even more serious when the object of authentication is in the form of electronic evidence that is produced, transformed, or manipulated with *artificial intelligence*. Electronic evidence is not only in the form of data that is easy to copy and move, but can also be in the form of digital representations that

[17] P. J. Alamsyah, K. Komarudin, D. Junaedi, R. A. A. Fikri, and F. F. Yusmar, "The Role of Electronic and Digital Forensic Evidence Methods in Modern Criminal Law Enforcement in Indonesia," *Indonesian Journal of Printing 5, no.* 3 (2026): 1028–38, https://doi.org/10.58344/jii.v5i3.7618.

visually and auditorially appear identical to the real facts. Generative *AI technology* allows the creation or modification of images, videos, sounds, and text with a higher level of resemblance to the original object.[18] These developments have prompted the attention of judicial institutions in various jurisdictions as AI-generated media has become increasingly difficult to distinguish from authentic media, while detection methods do not always provide conclusive guarantees. This uncertainty is exacerbated by the unwillingness to explicitly admit AI-based evidence in the conventional evidentiary paradigm adopted by the Criminal Procedure Code and the ITE Law, thus creating a legal vacuum that has implications for the legitimacy, accountability, and fairness of the parties.[19] This threat creates an epistemic problem in evidentiary law: it is not enough for the court to know that a *file* is available, but must be able to determine whether it comes from the claimed source, remains intact since it was obtained, has not undergone manipulation that changes its meaning, and has a verifiable control process.

The construction of Article 235 of the Criminal Procedure Code shows that the lawmakers have placed authentication as an important prerequisite for the use of evidence. The problem arises because the norm mainly determines authority, not capacity and methodology. Article 235 paragraph (4) specifies that judges have the authority to assess authentication, but does not establish the standards of technical examination that must be used to assess the authenticity of electronic evidence. The norm also does not regulate circumstances when judges do not have sufficient technical knowledge to identify digital manipulation, does not specify when forensic digital examinations become mandatory, and does not establish mechanisms that ensure the availability of digital forensic experts when the authenticity of evidence is disputed. The vacuum results in an imbalance between normative obligations and institutional capacity: judges are required to be *authentication gatekeepers*, but the system has not explicitly ensured that such *gatekeepers* have access to the knowledge and instruments necessary to perform those functions.

This condition can be analyzed through Soerjono Soekanto's theory of law enforcement effectiveness. Soekanto explained that the success of law enforcement is influenced by five interrelated factors, namely legal factors, law enforcement factors, facilities or facilities factors, community factors, and cultural factors.[20] This theory is important because the existence of norms that textually give authority to judges does not automatically indicate that the authority is effective. Legal effectiveness requires that there is a conformity between the norms that give mandates, the apparatus that carries out the mandate, and the means that allow the mandate to be implemented. Soekanto's perspective thus shifts the analysis from the question of whether Article 235 of the Criminal Procedure Code has regulated

[18] S. A. Fahlani, E. T. Rahman, M. A. Ilmy, and A. Mursal, "The Position and Evidentiary Strength of Deepfakes in the Trial Process," Shilap Journal of Lepidopterology, 2026, https://doi.org/10.31602/al-adl.v18i1.18914.

[19] M. N. S. Dewi and M. Muslem, "The Validity of Artificial Intelligence Evidence in the Judicial System: A Juridical Analysis," *Journal of Sharia Jurisprudence of Islamic Economic Legislation* 17, no. 2 (2025): 320–334, https://doi.org/10.32505/jurisprudence.v17i2.11022.

[20] S Humulhaer, "The Harmonization of Law Enforcement in the Eradication of Criminal Acts of Corruption," *Journal of Law Reform* 10, no. 2 (2023): 203, https://doi.org/10.26532/jph.v10i2.31329.

authentication to a more substantive question, namely whether the judicial system has the capacity to carry out authentication correctly.

Law enforcement factors are the first determining issue. Judges have primary competencies in law, juridical reasoning, fact-finding, and the application of evidentiary norms, but these competencies do not automatically include technical competencies in the fields of informatics, artificial intelligence, cybersecurity, metadata analysis, or *digital forensics*. Electronic evidence authentication involving alleged AI manipulation may require an examination of metadata, *file* structure, device sources, trace changes, *hash value*, *digital provenance*, compression patterns, audio-visual characteristics, and the possible use of generative models. These examinations are technical issues that require specialized knowledge and testable methods. A judge cannot be positioned as a technologist simply because the law gives him the authority to assess authentication.

This does not mean that the judge loses the authority to determine authentication. Legal authority and technical competence are two different things. The judge remains the party who has the judicial authority to determine whether evidence is admissible and how its evidentiary value is, while technical examination can be given to experts who have special competence. The concept of *judicial gatekeeping* in the development of modern evidentiary law actually shows that judges need the help of scientific knowledge when it comes to assessing technical evidence. In *the framework of Daubert*, for example, judges are placed as *gatekeepers* who assess the relevance and reliability of scientific evidence, but these assessments are built through examination of methods, scientific basis, error rates, and application of methods by experts.

The need for expert knowledge is becoming clearer because the issue of digital authentication is not always a problem that can always be solved through direct observation. A judge can see a video, listen to a voice recording, or read a digital conversation, but that perception cannot ensure that the material is authentic. A natural-looking video can be a *deepfake*, a voice that sounds identical to a person can be the result of *voice cloning*, and the appearance of a conversation on a messaging app can be engineered without representing the actual communication. Human perception-based judgment therefore has limitations when the object of proof has been produced by technology designed to mimic reality. The literature on the assessment of scientific evidence even shows the paradox that judges who function as *gatekeepers* may have more limited knowledge than experts whose knowledge they have to evaluate.

The issue of competence is not just a theoretical assumption. Empirical studies of *judicial gatekeeping* show that judges can have difficulty understanding scientific concepts and applying reliability criteria when dealing with technical evidence. A survey of 400 state court judges, for example, found that only 4% of respondents showed a correct understanding of the concept of *error rates*.[21] The findings confirm that the granting of *gatekeeping* authority does not automatically result in accurate scientific evaluations. The implications are relevant for Indonesia's evidentiary system because AI technology produces even more complex problems than simply assessing expert testimony about established science. Judges must face questions regarding the origin of the data, the integrity of *the files*, the methodology for detecting manipulations, the rate of algorithm errors, and the possibility of new methods of manipulation that are not yet widely known.

The factor of facilities or facilities in Soerjono Soekanto's theory is the second problem that shows the inadequacy of Article 235 of the Criminal Procedure Code. Soekanto places facilities or facilities as a decisive element because law enforcement cannot run effectively without highly educated and skilled human resources, good organization, adequate equipment, and necessary institutional support.[22] This conception has direct relevance to the authentication of electronic evidence. The court cannot produce reliable authentication if there is no digital forensic laboratory, adequate examination devices, data preservation systems, metadata analysis tools, hash verification capabilities, chain of custody *examination mechanisms*, and experts who are able to explain the results of the examination to the judge.

The absence of such facilities results in a problem that is different from simply a lack of regulation. Norma can order judges to assess authentication, but these orders do not result in reliable authentication if the object being examined has never gone through an adequate technical examination process. This situation can be described as *normative empowerment without institutional enablement*: judges are given normative authority, but are not always given institutional tools that allow this authority to be used effectively. This gap between *legal authority* and *institutional capacity* is why Article 235 of the Criminal Procedure Code has not sufficiently guaranteed the reliability of electronic evidence.

The need for digital forensic facilities is growing stronger because modern authentication does not stop at the question of whether a *file* can be opened or displayed in court. *Forensic authentication* must be able to answer at least questions about who created or acquired the data, when the data was created, whether the data has changed, how the data was transferred, and whether the material submitted is truly the same as the original source. The guidelines discussed in the United States judicial environment distinguish *forensic verification*, which focuses on determining whether a piece of content is created or manipulated by AI, from *forensic authentication*, which focuses on the origin and integrity of the content. This distinction is important for Indonesia because authentication in Article 235 of the

[21] J. V. Pergolizzi and J. A. LeQuang, "Black Robes and White Coats: Daubert Standard and Medical and Legal Considerations for Medical Expert Witnesses," *Cureus* 16, no. 9 (2024), https://doi.org/10.7759/cureus.69346.

[22] S Setiadi, "Optimization of Humanist Law Enforcement in Order to Realize the Paradigm of Civilian Police," *Unnes Law Journal* 9, no. 1 (2023), https://doi.org/10.15294/ulj.v9i1.66846.

Criminal Procedure Code should not be understood only as a formal check of the existence of a *file*, but as a process to ensure the reliability of the digital representation used to prove the facts.

The condition of Indonesian judicial practice shows the urgency of this problem. A review of court decisions shows that there are differences in the application of electronic evidence authentication checks; some cases receive electronic evidence without comprehensive forensic digital verification, while others use forensic examination to ensure the authenticity and integrity of evidence. The absence of operational standards for digital forensic procedures has been proven to cause inconsistency in the assessment of evidence in court, threaten legal certainty, and open up opportunities for violations of the rights of defendants.[23] Other research also identified the lack of a coherent legal architecture for electronic evidence in the new Criminal Procedure Code and the fragmentation of digital forensic standards in Indonesian criminal evidence.[24] These variations show that the issue of authentication is not only related to the individual capabilities of judges, but also to the lack of institutional infrastructure that ensures that electronic evidence examinations are carried out with relatively uniform standards.

The problem becomes more complex as the development of AI creates what can be called *epistemic displacement* in criminal evidence. In conventional evidentiary systems, judges can use experience and reasoning to assess whether a representation of facts makes sense. Generative technology disrupts this relationship because something that appears to be real is not necessarily a representation of a real event. Visual evidence is no longer always identical to factual evidence, whereas audio evidence is no longer always identical to the voice actually produced by the person whose name is associated with the recording. This risk creates two equally dangerous possible mistakes, namely accepting false evidence as authentic or rejecting authentic evidence because it is considered the result of AI manipulation. The latest literature calls these two threats fabrication *threats* and *liar's dividends*.[25]

This threat shows that the reliability of proof cannot be equated with formal legality. Electronic evidence can meet the requirements for formal submission but still has the problem of material authenticity. On the other hand, evidence that is substantially authentic can lose its probative value if the process of obtaining and mastering it cannot be verified. The difference between *admissibility*, *authenticity*, *integrity*, and *probative value* therefore needs to be maintained conceptually. Article 235 of the Criminal Procedure Code has linked authentication to *admissibility*, but has not provided sufficient technical parameters to ensure that the conclusion regarding authentication is truly based on a *reliable* method. Thus, normative

[23] D. Fernando, D. D. Heniarti, and C. A. F. Zakaria, "Transformation of Electronic Evidence Using Digital Forensics in the Reform of Criminal Procedure Law," *Journal of Justiciabelen (JJ) 5, no.* 1 (2025): 60, https://doi.org/10.35194/jj.v5i01.5506.

[24] P. Dickson, M. Manuputty, and Y. P. Ginting, "The Evidentiary Power of Digital Conversations as Unregulated Evidence in the Criminal Code," *Journal of Law and Human Rights Sciences* 4, no. 3 (2025): 521–35, https://doi.org/10.58812/jhhws.v4i03.2727.

[25] O Shamov, "From Synthetic Reality to Judicial Reality: Procedural Challenges of 'Deepfakes' and Their Solutions in the Age of Artificial Intelligence," *Entrepreneurship Economics and Law, no.* 3 (2024): 51–55, https://doi.org/10.32849/2663-5313/2024.3.09.

recognition of electronic evidence has not been accompanied by adequate technical parameters to determine its reliability.

Lawrence M. Friedman's perspective on the legal system strengthens this analysis through the distinction between *legal substance*, *legal structure*, and *legal culture*.[26] The legal substance in Article 235 of the Criminal Procedure Code has provided the basis for recognition and authentication authority. The legal structure requires judges, courts, experts, laboratories, and supporting institutions capable of translating these norms into verifiable examination practices. Legal culture demands the acceptance that electronic evidence should not be trusted just because it appears convincing, but should be treated as an object that requires verification when its authenticity is in question. Weaknesses in the legal structure cause relatively progressive substances to not fully produce reliable evidence.

Lon L. Fuller's thoughts on the *inner morality of law* are also relevant to look at the issue from a different perspective.[27] It is not enough for the law to have rules that order something, but it must provide the conditions that allow the rules to be implemented consistently. The obligation of judges to assess authentication without a mechanism that ensures the availability of knowledge and examination instruments can create a gap between norms and implementation. Norms that give authentication authority to judges must be accompanied by procedures and institutions that allow such authority to be exercised rationally. The reliability of proof is thus a matter not only of the content of the rule, but also of the ability of the legal system to provide operational conditions for the application of the rule.

This argument can be sharpened through the view of the judge as *a gatekeeper*. The *gatekeeping* function has the consequence that the judge not only accepts the evidence submitted by the parties, but must screen its relevance and reliability. *The Daubert* system shows that the function is not designed to make the judge a scientist, but to provide a mechanism so that the scientific and technical evidence that enters the trial has a methodological basis that can be accounted for. The problem with Article 235 of the Criminal Procedure Code lies in the absence of an architecture that explains how *gatekeeping* of electronic evidence is carried out when the judge faces technical problems that cannot be solved through legal knowledge alone. The risk of *idiosyncratic authentication*, i.e. differences in authentication assessments that depend on the individual capacity of judges and the support available in individual courts, become increasingly open when technical standards are not yet uniform. The literature on *gatekeeping* even warns that broad authority without a uniform methodology can result in disparities in decisions regarding *admissibility*.

This situation shows that the main problem of Article 235 of the Criminal Procedure Code does not lie in the absence of textual authentication arrangements. Instead, it has provided a fairly clear recognition of the necessity of authentication and the judge's authority to assess it. The inadequacy lies in the *operational architecture of authentication*, namely the absence of adequate arrangements

[26] H. S. Flora, M. T. H. Thuong, and R. D. Erawati, "The Orientation and Implications of New Criminal Code: An Analysis of Lawrence Friedman's Legal System," *IUS Journal of Law and Justice Studies* 11, no. 1 (2023): 113–25, https://doi.org/10.29303/ius.v11i1.1169.

[27] Lon L. Fuller, The Morality of Law, Revised Edition (New Haven: Yale University Press, 1969), pp. 33–38.

regarding technical competence, the involvement of digital forensic experts, examination standards, examination facilities, and verification procedures that must support the judge's authority. Soerjono Soekanto's perspective shows that these weaknesses mainly arise in law enforcement factors and facilities or facilities. Judges as law enforcers have not been institutionally positioned with adequate technical competence support, while the means and facilities to examine digital evidence have not been made an explicit part of the authentication design in the Criminal Procedure Code.

The adequacy of the authentication arrangement must therefore be assessed not on the basis of the existence of the word "authentication" in Article 235 of the Criminal Procedure Code, but on the ability of the entire system to produce an accountability decision. This measure requires a relationship between norms, competences, experts, technology, procedures, and judicial decisions. Judges must remain legal decision-makers regarding authentication, but these decisions need to be supported by technical examinations conducted by parties with special competence. Digital forensics in this context is not just an investigative tool, but part of an epistemic infrastructure that allows courts to distinguish authentic data from data that has been manipulated.

This inadequacy is increasingly evident in the context of *artificial intelligence*. The development of AI moves dynamically, while criminal procedure law tends to change more slowly. Recent research even shows that the existing evidentiary frameworks in various jurisdictions face problems when AI manipulation becomes increasingly difficult to distinguish from authentic media. Indonesia faces the same problem with additional institutional problems in the form of non-uniform digital forensics standards and the lack of special parameters to assess evidence made or modified by AI. This situation causes the authority of judges based on Article 235 paragraph (4) of the Criminal Procedure Code to potentially develop normatively faster than the institutional capacity that supports it.

Based on the overall analysis, the regulation of electronic evidence authentication in Article 235 of the Criminal Procedure Code is not enough to guarantee the reliability of criminal evidence in the era *of artificial intelligence*. The inadequacy is not because the Criminal Procedure Code completely ignores authentication, but because authentication is still formulated as judicial authority without being equipped *with a supporting architecture* that guarantees the capacity of law enforcement and the adequacy of examination facilities. The law enforcement factor in Soerjono Soekanto's perspective shows that there is a limitation of the technical competence of judges to authenticate independently, while the factor of facilities or facilities shows the need for digital forensic experts, examination devices, laboratories, and technical procedures that can verify the integrity and provenance of electronic evidence. This gap has caused Article 235 of the Criminal Procedure Code to only achieve formal recognition of authentication, but it has not fully achieved *institutionally supported reliable authentication*.

This construction also shows the need to change the authentication paradigm from judges as authenticity checkers to judges as judicial gatekeepers supported by digital forensic authentication mechanisms. Such a model does not reduce the independence of judges and does not hand over the authority of proof to experts. Experts provide technical bases regarding authenticity, integrity, provenance, and

possible manipulation, while judges determine the legal consequences in the framework of admissibility and probative value. This reconstruction is necessary so that Article 235 of the Criminal Procedure Code does not stop at granting authority to judges, but provides an institutional ecosystem that allows the authority to produce consistent, verifiable, and accountable authentication decisions. The reliability of criminal evidence in the era of *artificial intelligence* is ultimately not enough to be guaranteed by judges who have the authority to assess evidence, but requires a system that ensures that judges have adequate knowledge, expert assistance, and means to assess whether what appears to be evidence is really evidence.

Reconstruction of the Electronic Evidence Authentication Mechanism that can strengthen the capacity of judges to assess the authenticity of evidence that has the potential to be manipulated through *artificial intelligence*

The limitations of authentication arrangements in Article 235 of the Criminal Procedure Code show that the resolution of electronic evidence issues is not enough to be done through the addition of authority to the judge. Judges do have the authority to assess authentication based on Article 235 paragraph (4) of the Criminal Procedure Code, but this authority must be accompanied by a mechanism that allows judges to obtain a reliable technical basis. The reconstruction of the authentication mechanism therefore needs to be directed at the establishment of a system that integrates judicial authority, forensic digital examination, experts, verification technology, and procedural standards. The need for uniform standards is urgent because existing practices show that the mechanism for examining electronic evidence between agencies is still different and not uniform; these differences in methods have the potential to produce different findings and ultimately make it difficult for judges to make decisions. The most realistic normative instrument to build such a mechanism is the Supreme Court Regulation, while the technical instrument is in the form of an electronic evidence authentication application that is integrated with case administration in each court. The Supreme Court itself has previously used PERMA as an instrument to regulate the administrative and procedural aspects of electronic trials, including through PERMA Number 1 of 2019 and PERMA Number 4 of 2020.[28] PERMA Number 1 of 2019 concerning Electronic Case Administration and Trials in Court has been perfected through PERMA Number 7 of 2022,[29] while PERMA Number 4 of 2020 regulates the administration and trial of criminal cases electronically,[30] which was later amended by PERMA Number 8 of 2022.

This idea gained a stronger basis after the 2025 Criminal Procedure Code explicitly placed electronic evidence as evidence and gave authority to judges to assess its authenticity. The Supreme Court itself has affirmed that Article 235 of the

[28] M. Gerry and R. E. Rizkiana, "The Optimization Strategy of E-Courts Organizing Quality in Indonesia," *UNTAG Law Review* 7, no. 1 (2023): 11, https://doi.org/10.56444/ulrev.v7i1.3874.

[29] D. A Handayani, "The Effectiveness of E-Court Civil Cases during the Pandemic and Post-COVID-19 Pandemic in Makassar," *Legal Issues* 52, no. 2 (2023): 119–30, https://doi.org/10.14710/mmh.52.2.2023.119-130.

[30] H. B. Purnomo, R. H. S. Akili, and R. W. Amu, "Analysis of the Effectiveness of Electronic Criminal Trials," *Mutiara Journal of Research and Scientific Works* 2, no. 3 (2024): 69–79, https://doi.org/10.59059/mutiara.v2i3.1237.

2025 Criminal Procedure Code requires evidence to be proven to be authentic and gives authority to judges to assess its authenticity and legality. The need for derivative arrangements is in line with the findings of legal studies that until now there has been no explicit obligation for judges to authenticate electronic evidence through certain mechanisms, and there is no provision that guides judges on whether examinations are carried out directly through storage devices or through data duplication results.[31] Research prior to the birth of the 2025 Criminal Procedure Code has even identified the need for regulations in the form of PERMA to fill procedural law gaps related to electronic evidence and emphasize the importance of validation by parties with certified special knowledge and expertise. Juridical recognition of electronic evidence through the Criminal Procedure Code, the ITE Law, and Supreme Court regulations is only valid as long as its authenticity and integrity can be proven, while challenges in the form of potential data manipulation, limited infrastructure, and lack of competent human resources still persist.[32] This capacity issue is also reflected in the findings that judges still face challenges in authentication procedures, digital forensic capabilities, and consistency of legal standards.[33] These developments show that the idea of establishing PERMA is not an addition to a new evidentiary regime, but a form of operationalization of court authority to ensure that the authentication requirements in Article 235 of the Criminal Procedure Code can be implemented consistently.

The construction of PERMA needed to use a *forensically supported judicial authentication approach*. The concept places the judge as the final decision-maker regarding authentication, but the decision is supported by a technical examination conducted through a digital forensic system. This position is important to maintain the boundary between the function of the expert and the function of the judge. The expert does not determine whether a piece of evidence has probative power, while the judge does not take over the technical function of the expert. This separation of roles is in line with the concept *of judicial gatekeeping*, which places the judge as the party who supervises the entry of scientific arguments into the courtroom, while at the same time recognizing that individuals who are highly proficient in a discipline have a great influence on judges or jurors who may not have literacy in that scientific field. [34] The judge accepts the results of the technical examination as a basis for assessing whether the authentication requirements are met and then determining the legal consequences based on Article 235 paragraph (4) and paragraph (5) of the Criminal Code.

This construction is consistent with the concept *of judicial gatekeeping* in evidentiary law. Rule 901 *of the Federal Rules of Evidence*, for example, requires that

[31] W. Istiqomah, M. Sood, and Muh. Risnain, "Juridical Analysis of Electronic-Based Use Rights ~~Certificates: Study at Mataram City~~ National Land Agency Office, Indonesia," *Path of Science* 10, no. 1 (2024): 8034–45, https://doi.org/10.22178/pos.100-36.

[32] P. Achyarsyah, S. Riyadi, K. Widodo, and M. Chamim, "The Role of Digital Evidence in Criminal Law Enforcement: Challenges of Authentication and Admissibility in Court," *Research Horizon 5, no.* 6 (2025): 2987–98, https://doi.org/10.54518/rh.5.6.2025.950.

[33] R. S. Billah and H. Saragih, "Challenges of Cybercrime Law Enforcement for Judges from the Legal Aspect of Evidence in Indonesia," *Journal of Social and Humanities Flow 5, no.* 2 (2025): 2739–47, https://doi.org/10.57250/ajsh.v5i2.1543.

[34] E. Peruzzi and G. Cesar, "The Gatekeeper's Dilemma: Expert Testimony, Scientific Knowledge and Judicial Reasoning," *SSRN Electronic Journal* (2024), https://doi.org/10.2139/ssrn.4763570.

there be sufficient evidence to support the conclusion that an object is what the party claiming to be the one who filed it; within that framework, the court of first instance assesses whether the party presenting evidence has presented sufficient evidence to convince the jury that the object is indeed what it claims.[35] It also opens up the possibility of authentication through witnesses who know the object, expert opinions, comparisons with authenticated specimens, special characteristics, and other methods that can support identification. Developments in the literature on *deepfake evidence* have even prompted proposed changes to Rule 901 because traditional authentication methods are considered to face new challenges when evidence can be synthetically generated through AI; one proposal revises Rule 901(c) with a shifting evidentiary burden framework, i.e. when the denying party demonstrates a sufficient basis that AI manipulation has occurred, the party submitting evidence is required to authenticate the evidence and provide additional evidence regarding its reliability.[36] Another proposal leads to two new rules of evidence submitted to the Rules of Evidence Advisory Committee to respond to challenges to AI-generated evidence, both recognized and unrecognized as AI-generated results.[37] These experiences can serve as a benchmark for Indonesia without having to adopt them raw.

The proposed PERMA can be given a normative construction as a PERMA on Procedures for Authentication Tests and the Validity of Electronic Evidence in Criminal Cases. The terminology of "authentication test" needs to be distinguished from "evidentiary strength assessment". The authentication test aims to ensure the identity, origin, integrity, and condition of an electronic evidence before the evidence is used as a basis for proof. The assessment of the strength of proof remains the judge's territory in deciding cases. This distinction is important so that the application of authentication does not turn into *an automated adjudication* and does not shift the judge's constitutional authority in assessing facts and law. The need for a clear division of roles between judges and technical experts is also reflected in the findings that the burden of proof and the role of information technology experts are still unclear in practice, so the adoption *of digital chains of custody* and verified electronic signatures is the recommended step.[38]

The PERMA needs to contain at least eight main components. The first component is the scope of authentication objects which includes photographs, videos, voice recordings, electronic conversations, electronic documents, electronic mail, electronic transaction data, application data, surveillance camera recordings, metadata, *cloud data*, and other forms of digital evidence. The second component is the subject who can submit evidence, including investigators, public prosecutors,

[35] J Yu-Mi, "Deepfake Evidence and Its Authenticity in U.S. Criminal Trials," *41, no.* 3 (2025): 65–86, https://doi.org/10.22397/wlri.2025.41.3.65.

[36] A. L Martinez, "Jurisvision of Deepfake Financial Documents: Semiotic Disruption and Remediation in Post-Textual Evidence," *International Journal for the Semiotics of Law, June* 3, 2026, https://doi.org/10.1007/s11196-026-10514-w.

[37] M. Grossman and P. Grimm, "Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence," *Science and Technology Law Review* 26, no. 2 (2025), https://doi.org/10.52214/stlr.v26i2.13890.

[38] K. D. Kusnadi and S. A. Wiraguna, "Legal Development for Electronic Evidence in Civil Litigation: Challenges and Future Expectations," *SENTRI Journal of Scientific Research* 4, no. 12 (2025): 3866–70, https://doi.org/10.55681/sentri.v4i12.5102.

defendants, legal counsel, victims, witnesses, and other parties who are legally authorized to submit evidence. The third component is the initial admission and preservation procedures. The fourth component is forensic digital examination, which in practice demands the standardization of electronic evidence management because digital evidence is easily manipulated by cybercriminals.[39] The fifth component is the analysis of indications of manipulation or synthetic production through AI, which is necessary due to the barriers to digital forensic proof and the limited capacity of law enforcement in verifying AI-based content as part of the ineffectiveness of law enforcement, so that affordable digital forensic reinforcement becomes a necessity.[40] The sixth component is the creation of electronic authentication reports, which can utilize integrity verification techniques such as metadata analysis, digital signatures, and *watermarks* to assess the integrity of the image and its derivative versions. The seventh component is the mechanism of examination and objections of the parties. The eighth component is the judge's decision regarding authentication and the consequences of its proof.

The stages in the PERMA make the following pattern:

1. Electronic Evidence Submission Stage

Each electronic evidence obtains an Electronic Evidence Identification Number (EEIN) as a unique identity. The system records who submitted the evidence, the date and time of receipt, the form of storage media, file size, file format, device source, and the party responsible for submitting the evidence. The data becomes part of the *chain of custody*. Every move, access, examination, or extraction of evidence is recorded in the system so that it can be known who accessed the data and for what purpose. The mechanism transforms the *chain of custody* from just an administrative document to a *verifiable* digital audit trail.

2. Forensic preservation stage

The original evidence must not be directly analyzed through a device that allows changes to the file. The system must create a forensic copy or *forensic image* and calculate the hash value of the original object as well as the forensic copy. The slightest change to the data can be tested through a comparison of the hash value. The check must maintain the original object in a *read-only condition* so that the analysis is performed against the forensic copy. The concept reinforces the principle of integrity because the question of authentication does not stop at "does the file look genuine", but moves on the question of whether the file being examined remains identical to the file that was first obtained.

3. Metadata examination stage

Authentication applications must display the available metadata of each digital object. Photo metadata can include the creation time, device, operating system, coordinates if available, format, size, resolution, and other technical parameters. Video metadata can include the recording device, duration, *frame rate*, codec, creation time, format changes, and other available technical information. Audio

[39] C. Monique, Y. Yuliati, and F. Sulistio, "Exploring the Role of Digital Forensics in Identifying Cyber Crime in Indonesia's Criminal Procedure Law," *Pena Justisia: Media Communication and Legal Studies* 23, no. 2 (2024): 825, https://doi.org/10.31941/pj.v23i2.4068.

[40] S. Nurkholisah, D. Rismana, A. E. Nugroho, A. Munjiyah, and Q. Ayunisa, "Deepfakes as a New Form of Cybercrime: Challenges of Criminalization in Indonesian Criminal Law," *Journal of USM Law Review* 8, no. 3 (2025): 2421–45, https://doi.org/10.26623/julr.v8i3.13060.

metadata can include format, *sample rate*, *bit depth*, recording device, and encoding parameters. Document metadata can include creation time, modification time, application used, *author information*, and technical history that is still recoverable. Metadata checks should not be treated as single proof of authenticity because the metadata itself can be modified. Metadata should be positioned as one of the layers of information that is correlated with the results of other checks.

4. Provenance verification stage

Systems need to answer questions about where the evidence came from and how it got to the courts. Provenance checks can compare device information, metadata, *hashes*, creation time, storage sources, user accounts, and data transfer records. This approach is in line with the development of technical standards that place content authentication and provenance tracking as two critical components in dealing with synthetic content. NIST specifically identifies authentication, provenance tracking, synthetic content labeling, synthetic content detection, and software testing as important approaches in improving digital content transparency.

5. AI-manipulation analysis stage

Court applications need to have modules that analyze whether an object shows indicators of production or manipulation using *artificial intelligence*. The module can test *synthetic media artifacts*, temporal inconsistencies, compression anomalies, metadata mismatches, *face synthesis* characteristics, sound manipulation, *lip synchronization* anomalies, *frame inconsistency*, as well as other indicators relevant to the type of media. The system can also use multiple detection engines simultaneously so that the results do not depend on a single algorithm. This approach is safer than using one *AI detector* because deepfake detection has *false positives* and *false negatives*. NIST itself emphasizes that media analysis systems need to be tested using authentic media and manipulated media and must know the level of detection errors.

The application should not produce simple conclusions in the form of "AI" or "non-AI". A more appropriate output is forensic risk assessment with categories such as *no significant manipulation indicator detected*, *potential manipulation detected*, *probable synthetic generation*, or *inconclusive*. Each result should be accompanied by the underlying indicator, the examination method used, the version of the algorithm, the level of trust, the level of known error, and a recommendation on whether a manual examination by an expert is required. This approach is important because AI technology is constantly evolving and no detection technology can provide absolute guarantees. Recent developments even show that judicial stakeholders still face limitations in detecting synthetic media and there is no detection method that can be considered always perfect.

The concept of human-in-the-loop needs to be a fundamental principle. The outcome of the application should not be binding on the judge and should not be the only basis for declaring evidence inauthentic. NIST itself recommends that algorithmic analysis and automated decision-making be complemented by manual checks to address detection errors. Such models can be applied in court systems through escalation mechanisms. Evidence with low risk can obtain automated reports, while evidence that shows indications of manipulation, metadata conflicts,

or a high level of uncertainty must be forwarded to a digital forensic expert for further examination.

6. Expert verification stage

The court needs to have a unit or network of digital forensic experts who meet certain competency standards. These experts can come from within the judicial institution or from other institutions that meet the requirements of independence and competence. PERMA must set standards regarding qualifications, certification, independence, documentation obligations of examination methods, and expert responsibility. The system avoids judges from the position of having to determine technical issues based on personal knowledge. Previous Supreme Court studies have led to the need for validation of electronic evidence by parties with special knowledge and expertise and suggested the establishment of PERMA regulations.

Thus, there is no longer a mechanism for each to prove by being corroborated by their respective experts, then the judge considers. This is because the judge does not have the knowledge, experience and skills to assess the validity of electronic evidence. Thus, the court must have its own experts in determining the validity. In the case of corruption, both the Public Prosecutor and the Defendant may submit an expert to recalculate the state loss, but it must not find a point of understanding, thus based on Article 6 of the Supreme Court circular letter Number 4 of 2016, the judge in adjudicating corruption cases obtains the authority to assess the state's losses based on the facts of the trial, so it is strengthened by Article 235 paragraph (4) of the ICC, then the judge determines the validity.

7. Authentication Hearing Stage or Special Examination of Authentication If the Authenticity of Evidence is Disputed.

The examination does not always have to be conducted as a separate trial. The judge may determine that the issue of authentication must be examined first before the evidence is used to prove the subject matter. The party who submits evidence is given the opportunity to explain the source, how it was obtained, and the integrity of the evidence. The opposing party is given the right to test the authentication method, question the *chain of custody*, present comparative experts, and point out possible manipulation. The judge then makes a determination about the status of authentication based on all available information.

8. Judicial authentication decision stage

The judge can determine at least four statuses: authentic, inauthentic, authentic with limitations, or undeterminable. The "authentic with limitations" status is important because digital evidence is not always in a black-and-white state. A file can be proven to be from a specific device but undergoes a compression process after submission. A video can be proven to be from a specific camera but certain parts can be edited. A sound recording can be authentic as a file but does not necessarily prove the identity of the person who produced the sound. The distinction between the authenticity of an object and its evidentiary value allows the judge to avoid the overriding conclusion that the authenticity of an automatic file proves the truth of the entire contents of the file.

The framework can be formulated in the Eight-Layer Electronic Evidence Authentication model, namely:

Stages	Mechanism	Output
1	Registration	Unique identity of evidence/EEIN
2	Preservation	Original evidence and forensic copy
3	Hash Verification	Ensuring the integrity of files
4	Metadata Examination	Technical information and file history
5	Provenance Analysis	Origins and flow of mastery
6	AI Manipulation Detection	AI production/manipulation indicators
7	Expert Verification	Digital forensic opinion
8	Judicial Authentication	Judge's determination on authentication

The model basically changes the mechanism of Article 235 of the Criminal Procedure Code from single-point judicial authentication to multi-layer authentication. Article 235 paragraph (4) still places the judge as the authority to assess authentication. The technical layer provides an epistemic basis for the exercise of this authority. This structure creates a more rational relationship between law and technology because it does not require judges to do work that is methodologically the field of digital forensics.

Soerjono Soekanto's perspective on law enforcement factors provides theoretical legitimacy for the reconstruction of the proposed authentication mechanism. Law enforcement factors and facilities cannot be separated in implementing Article 235 of the Criminal Procedure Code. The authority of judges as law enforcement requires competency support and technical resources so that authentication norms can be applied effectively. Soekanto's literature on factors that affect law enforcement does place law enforcement and facilities as factors that determine the effectiveness of legal work; facilities and facilities are positioned as tools to achieve legal effectiveness, while law enforcement officials are considered reliable if they have good professional skills and mentality. [41] Reconstruction through PERMA and its applications is thus not just a technological innovation, but a response to the gap between *legal authority* and *institutional capacity*.

Lawrence M. Friedman's perspective on *the legal system* reinforces this construction. Friedman's framework that distinguishes the substance of law, institutional structure, and legal culture has been used to assess the effectiveness of procedural law reform in Indonesia, and the analysis shows that procedural law reform still faces normative, structural, and cultural constraints.[42] The legal substance is contained in Article 235 of the Criminal Procedure Code which establishes authentication obligations. The legal structure includes judges, courts, forensic digital experts, system administrators, and supporting institutions. Legal

[41] N. N. Vidyapramatya, E. Latifah, E. Farida, and A. A. Tigor, "Authority of the Dispute Council in the Resolution of Construction Disputes in Indonesia," *Law Reform* 19, no. 1 (2023): 88–109, https://doi.org/10.14710/lr.v19i1.49141.

[42] Y. P. Ginting, A. C. G. Tumbelaka, B. D. Paulin, B. Natanael, E. J. Tiasono, E. Hamonangan, M. Cahaya, M. Samy, M. C. Darmawan, and Z. N. Firliyani, "The Application of E-Litigation in Civil Cases as a Form of Civil Procedural *Law Reform* in Indonesia," *Journal of Law and Human Rights Wara Ciencias* 4, no. 3 (2025): 491–502, https://doi.org/10.58812/jhhws.v4i03.2723.

culture requires all judicial actors to abandon the assumption that digital display is identical to factual truth. Since the constraints on these three aspects cannot be solved separately, they need to be linked simultaneously.[43] PERMA functions to connect these three dimensions through operational rules that transform abstract norms into a consistent inspection mechanism.

Lon L. Fuller's perspective on *the inner morality of law* is also relevant because law must provide conditions that allow rules to be applied consistently. Fuller views law as a moral enterprise that demands the fulfillment of a number of internal elements, namely generality, announcement, non-retroactivity, clarity, consistency, congruence, and feasibility of implementation, because these elements are considered to determine the legitimacy and effectiveness of a legal system.[44] An order to a judge to assess authentication without providing procedures, experts, and examination facilities will create a gap between *law in books* and *law in action*. PERMA can fill the operational space without changing the substance of the judge's authority that has been granted by the Criminal Code. The norm at the legal level provides a mandate, while PERMA provides procedures for the implementation of the mandate in the judicial environment.

The gatekeeping perspective in evidentiary law provides an important comparative dimension. Rule 901 *of the Federal Rules of Evidence* indicates that authentication is a process to provide a sufficient basis for the conclusion that the evidence presented is indeed the object claimed by the applicant. Developments regarding *deepfakes* indicate the need to adapt these mechanisms to synthetic evidence. A review of the existing evidentiary regime concludes that the law must be improved at the authentication stage before recorded evidence is accepted, including through changes in assumptions regarding *the admissibility* of such evidence. [45] Rebecca Delfino even proposed the development of Rule 901 to respond to the specific characteristics of AI-generated evidence.[46] Indonesia does not have to imitate the United States approach, but it can take its basic principle that *authentication* requires *a gatekeeping mechanism* that is proportionate to the risks of the technology.

[43] Y. P. Ginting, A. C. G. Tumbelaka, B. D. Paulin, B. Natanael, E. J. Tiasono, E. Hamonangan, M. Cahaya, M. Samy, M. C. Darmawan, and Z. N. Firliyani, "The Application of E-Litigation in Civil Cases as a Form of Civil Procedural *Law Reform* in Indonesia," *Journal of Law and Human Rights Wara Ciencias* 4, no. 3 (2025): 491–502, https://doi.org/10.58812/jhhws.v4i03.2723, 493.

[44] B. T. Bawono and H. Glaser, "The Urgency of Restorative Justice Regulation on Hate Speech," *Governance* 11, no. 2 (2024): 364, https://doi.org/10.20961/governance.v11i2.82508.

[45] Y. B Dissanayake, "Reforming Sri Lankan Law to Address Deep Fakes: Ensuring Admissibility of Contemporary Recordings in Evidence," *KDU Journal of Multidisciplinary Studies* 7, no. 2 (2025): 1–9, https://doi.org/10.4038/kjms.v7i2.201.

[46] Rebecca Delfino, "Deepfakes on Trial 2.0: A Revised Proposal for a New Federal Rule of Evidence to Mitigate Deepfake Deceptions in Court," *Loyola Law School, Los Angeles Legal Studies Research Paper No. 2025-10, February* 15, 2025, https://doi.org/10.13140/RG.2.2.12632.61447. Available at SSRN: https://ssrn.com/abstract=5188767.

The construction of authentication applications must also pay attention *to the principle of technological neutrality*. This principle demands that legislation does not favor or discriminate against certain technologies, but rather focuses on the effects or functions of the technology broadly, so that the rules can persist as technology changes.[47] PERMA should therefore not establish one brand of device, one algorithm, or one AI detection technology as the only standard. The technology used for manipulation will continue to evolve and detection methods may become obsolete. PERMA should set the parameters of the results that must be obtained, while the technical methods can be developed through operational standards, system updates, and periodic evaluations. The need for standardization is reflected in the role of standardization agencies such as *the National Institute of Standards and Technology* and *the Scientific Working Group on Digital Evidence*, which work toward consistent definitions and standards so that *deepfake* detection tools are uniformly applied and the results are trustworthy.[48]

The principle *of algorithmic accountability* should also be embedded in PERMA. Any automated examination results should be traceable to the algorithm, software version, relevant dataset or test base, examination parameters, and known error rates. The system should not provide *black-box conclusions* without an examineable reason. Judges and parties should be able to know why the system gives certain indications of manipulation. Such transparency is important because decisions regarding authentication can affect *admissibility* and ultimately affect the rights of the defendant. A study on the use of AI-based judicial assistants in Indonesia shows that reliance on algorithms with opak characteristics, as reflected in the COMPAS case in the United States, has the potential to violate the right of defendants to explanation and threaten the independence and discretion of judges.[49]

The application architecture can be built in the form of *an Electronic Evidence Authentication System* that is integrated with the Supreme Court's electronic case administration system. Each piece of evidence acquires a unique digital identity. The system hashes, reads metadata, stores *provenance*, records *the chain of custody*, executes manipulation analysis, and generates *an Authentication Report*. The report becomes an electronic document that can be examined by the judge and the parties. The system does not replace the trial, but provides an *evidence intelligence layer* that strengthens the quality of information available to the judge.

The scheme of work can be described as follows:

Electronic Evidence Submission → EEIN → Preservation → Hashing → Metadata Extraction → Provenance Verification → AI/Manipulation Analysis → Risk

[47] A Ojanen, "Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act," *European Journal of Risk Regulation* 16, no. 4 (2025): 1440–55, https://doi.org/10.1017/err.2025.10024.

[48] Y.-C. Wu, S. J. Sohrawardi, C. R. Gerstner, and M. Wright, "Understanding and Empowering Intelligence Analysts: User-Centered Design for Deepfake Detection Tools," *April* 25, 2025, 1–26, https://doi.org/10.1145/3706598.3713711.

[49] A. D. Saputra, H. T. Irwanto, and N. Nurisnah, "Measuring Judicial Accountability in the Algorithmic Era: Juridical Implications of Using Judicial Assistants and Black Box Risks in Constructing Judgment Arguments," *SIGn Journal of Law* 7, no. 2 (2025): 958–73, https://doi.org/10.37276/sjh.v7i2.570.

Classification → Expert Review → Authentication Report → Examination of Parties → Judicial Authentication → Admissibility → Probative Value.

The end result of such a mechanism must clearly distinguish between "AI-generated", "AI-assisted modification", "digitally modified", and "inconclusive". The "AI-generated" classification indicates a strong indicator that the whole or substantial part of the content is synthetically generated. The "AI-assisted modification" classification indicates an indicator that AI is being used to alter a particular part of an object. The "digitally modified" classification indicates the existence of a digital change but the method or source of the change cannot be ascertained as AI. The "inconclusive" classification indicates that the available evidence does not yet allow for an accountable conclusion. The classification is much more scientific than the "true/fake" binary system.

This construction also provides protection against *false authentication* and *false rejection*. *False authentication* occurs when evidence of manipulation is accepted as authentic, while *false rejection* occurs when actual evidence is rejected simply because the system detects possible manipulation. Both risks should be a concern because AI technology not only enables the production of false evidence, but can also create doubt on authentic evidence: widespread skepticism of visual media has the potential to make litigants reject evidence that is actually genuine, thus opening up space for parties who want to avoid accountability for their actions. [50] Conversely, the receipt of digital evidence without adequate verification has the potential to erode the principle of presumption of innocence, shift the burden of proof to the defendant, and undermine legal certainty.[51] Recent developments in the United States judiciary show that *the problem of deepfakes* has been seen as a threat to the court's function as *a gatekeeper*, while the available detection methods have not been able to provide absolute certainty.

PERMA also needs to regulate the parties' rights to algorithmic examination results. Defendants and legal counsel must have access to authentication reports, examination methods, metadata results, *hash values*, and expert conclusions as long as they do not interfere with the interests of the law. The public prosecutor also has the right to test results that declare the evidence presented to be inauthentic. The same right should be given to the party presenting evidence to present a comparative expert. This mechanism makes authentication an adversarial process that can be tested, not a technological decision that is automatically accepted. This issue is not just a theoretical construction: the jury's rejection of the defendant's voice recording on the grounds that the formal requirements and verification of the authenticity of the evidence have not been met has given rise to a juridical debate about the limits of the judge's authority to assess electronic evidence, as well as

[50] J. G. Twomey, D. Ching, M. P. Aylett, M. Quayle, C. Linehan, and G. Murphy, "Do Deepfake Videos Undermine Our Epistemic Trust? A Thematic Analysis of Tweets That Discuss Deepfakes in the Russian Invasion of Ukraine," *PLOS ONE* 18, no. 10 (2023), https://doi.org/10.1371/journal.pone.0291668.

[51] P. A. Rifqi, Samsidar, and H. C. J. Salmon, "Screenshots, Chats, and Voice Notes: Rethinking Evidence in Criminal Trials," *Journal of Criminal Justice* 2, no. 6 (2026): 43–51, https://doi.org/10.62872/0hb7ee97.

raising concerns that such refusal has the potential to limit the defendant's right to self-defense.[52]

PERMA also needs to regulate laboratory accreditation and expert competence. Each court has at least access to a regional forensic digital center that can provide technical examinations. Courts that have cases with high-risk digital evidence can request an examination from the center. A regional structure is more realistic than forcing each court to have a laboratory with the same level of sophistication. National standards are still set by the Supreme Court so that the results of examinations do not depend on the financial or technological capabilities of each court. This need is urgent because Indonesia only has around 147 certified digital forensic experts according to verified data in 2023 from the Indonesian Digital Forensics Association. [53] The limited capacity is in line with the finding that the expansion of judges' authority to assess the authenticity and legality of electronic evidence risks becoming ineffective, and even potentially causing criminal errors, if not accompanied by strengthening the technical competence of judges and providing supporting facilities in court.[54]

The institutional model can be formulated as *the Court Digital Evidence Authentication Center*. The unit does not act as a panel of judges and does not determine the value of evidence. The unit functions as a *forensic support institution* that conducts preservation, metadata extraction, integrity checks, *provenance analysis*, manipulation detection, and preparation of technical reports. The independence of the unit must be maintained so that the results of the examination are not under the control of the party who submits evidence. This structure strengthens the principle *of equality of arms* because both the prosecutor and the defendant can test the results of the examination through the same mechanism.

[52] A. T. A. Anshari, S. Januarita, M. Q. Dewani, J. M. Wijaya, W. S. Atmadja, and Y. P. Ginting, "The Evidentiary Power of Electronic Recordings as Testimony in the Perspective of Indonesian Criminal Law," *Sanskara Law and Human Rights* 4, no. 2 (2025): 181–91, https://doi.org/10.58812/shh.v4i02.698.

[53] EMN Setiawan and H. Hartiwiningsih, "Optimizing the Use of Digital Forensics and Information Technology in Proving Criminal Acts of Electronic Document Forgery in Indonesia," *International Journal of Law, Crime and Justice* 2, no. 2 (2025): 72–86, https://doi.org/10.62951/ijlcj.v2i2.587.

[54] M. Rustamaji, S.M. Sitompul, and A.R. Khoiruddin, "Reforming the Role of Judges in Assessing Evidence Authenticity and Legality: A Comparative Study Using the Exclusionary Rule Approach," *Media Iuris* 9, no. 1 (2026): 153–180, https://doi.org/10.20473/mi.v9i1.77218.

PERMA also needs to arrange for algorithm updates and system audits. The authentication system should not be considered complete after the application is launched. AI detection algorithms should be periodically tested against datasets consisting of authentic evidence, evidence of conventional manipulation, and proof of results of various *generative AI techniques*. The performance of the system should be measured through *false positive rate*, *false negative rate*, *precision*, *recall*, and other relevant parameters. Such testing demands a comparison between authentic media and manipulated media as well as documentation of the algorithm's error rate before the results are used as a basis for decision-making. This issue is closely related to transparency, because the reliance on algorithmic black *box systems* in criminal cases actually demands guarantees of the right to forensic algorithms that can be interpreted through court decisions and legislation.[55]

This construction resulted in an important paradigm shift. Conventional evidentiary systems tend to place the issue of authentication as a direct relationship between evidence and judges. Reconstructed systems place authentication as a verification ecosystem consisting of evidence, preservation, technology, experts, parties, and judges. Judges remain at the center of judicial decision-making, but no longer work in an isolated technical space. Technology provides information, experts provide technical interpretation, parties provide adversarial testing, and judges provide legal decisions.

Such reconstruction can be outlined in PERMA through at least the following normative structures: general provisions; authentication principles; classification of electronic evidence; registration and identification; preservation and *chain of custody*; metadata checks; integrity and *hash* checks; *provenance verification*; AI indication checks and digital manipulation; forensic digital expert standards; use of EEAS applications; *authentication reports*; examination of parties; judicial authority; classification of authentication results; objections and re-examinations; data protection; system security; algorithmic audits; technology updates; and transitional provisions.

The final construction offered by this research is thus not just "PERMA on electronic evidence", but PERMA on a digital forensics-based authentication test mechanism supported by the Electronic Evidence Authentication System. PERMA becomes a *legal framework*. Digital forensic laboratory becomes *technical infrastructure*. Experts become *scientific verifiers*. EEAS applications become *technological instruments*. Judges become *judicial gatekeepers*. Parties become *adversarial* controllers. These five elements form an authentication system that corrects each other.

The model can be summarized through the formula:

PERMA + DIGITAL FORENSICS + AI AUTHENTICATION SYSTEM + EXPERT VERIFICATION + JUDICIAL GATEKEEPING = RELIABLE ELECTRONIC EVIDENCE AUTHENTICATION.

The reconstruction provides an answer to the weaknesses of Article 235 of the Criminal Procedure Code. This provision does not need to be amended to give new authority to the judge because the authentication authority has been granted by paragraph (4). The main drawback lies in the lack of an operational mechanism that

[55] B.L. Garrett and C. Rudin, "Interpretable Algorithmic Forensics," *Proceedings of the National Academy of Sciences* 120, no. 41 (2023), https://doi.org/10.1073/pnas.2301842120.

connects the authority with technical capacity. PERMA can fill this space through the standardization of procedures, the establishment of digital forensic infrastructure, the arrangement of experts, and the implementation of electronic authentication systems. The application does not become a "digital judge", but rather an instrument that strengthens the quality of information used by judges to carry out *the gatekeeping* function.

The ultimate goal is not to create a system that claims to be able to determine the truth automatically. A more appropriate goal is to create a proof system that is able to provide a technical basis that is transparent, verifiable, testable by the parties, and accountable by the judge. The concept is more in line with the character of *artificial intelligence* because it does not assume that detection technology will always be perfect. The reliability of proof is built through a combination of layered examinations, openness of methods, expert verification, *human-in-the-loop*, adversarial rights of the parties, and the judge's final decision.

The model changes the principle of authentication from "the judge assesses whether the evidence is authentic" to "the judge assesses the authentication based on a verifiable verification process." The change is the core of the reconstruction. Article 235 of the Criminal Procedure Code has provided *legal authority*, while PERMA and the Electronic Evidence Authentication System provide *institutional and technological capacity*. Both are necessary so that the judge's authority does not stop as an abstract norm, but becomes a mechanism that is able to protect the integrity of criminal evidence when *artificial intelligence technology* is increasingly able to create digital reality that is difficult to distinguish from reality.

Reviewer-Driven Doctrinal Clarification and Evidentiary Limits

The proposed Electronic Evidence Authentication Standard (EEAS) should be treated as a procedural recommendation, not as existing Indonesian law. A PERMA could guide court-facing disclosure, hearing management and assessment of expert methods within its rule-making competence; it cannot be assumed to create new substantive offences, change statutory exclusion criteria or transfer the judge's decision-making authority to a forensic laboratory. Where a rule would alter the burden or content of legal proof, a legislative basis must first be established.

A proportionality-based examination rule is preferable to mandatory specialist testing of every electronic file. Heightened scrutiny should be considered where provenance is disputed, manipulation is plausibly alleged, the evidence is decisive, or an AI-origin warning is supported by independently verifiable circumstances. A detector's confidence score is not a legal authenticity verdict; reports should disclose validation dataset, tool version, known false-positive and false-negative limitations, drift risks, and whether a human specialist replicated the result. An inconclusive result does not reverse the criminal burden of proof or establish the accused person's guilt.

The institutional sequence should allocate collection and preservation to investigators; disclosure and case theory to the prosecution; challenge, independent testing and access to methods to the defence; technical explanation to competent experts; and the ultimate decision about legality, admissibility and weight to the court. An auditable EEAS requires access logs, signed transfers, hash-generation context, tamper-evident retention, change approvals and periodic independent review. Statements about the number or geographical distribution of accredited

Indonesian laboratories remain proposals for empirical verification unless supported by official capacity data.

Table: Legal analysis and evidentiary requirements (Article 736)

Question	**Forensic record**	**Decision responsibility**
What is the source?	Origin metadata, acquisition log and device/context	Investigator; challenge by defence
Has the file changed?	Hash plus demonstrably reliable baseline and custody chain	Expert assessment, judicial weight
Was acquisition lawful?	Warrant/consent and procedure as applicable	Court under Article 235
Is the content AI-manipulated?	Validated tools, uncertainty, replicable review	Expert explanation; court adjudicates
What if indeterminate?	State limits and unresolved hypotheses	Burden and fair-trial safeguards remain

Source: Authors' doctrinal synthesis based on the authorities identified in Article 736; missing primary evidence is labelled expressly.

CONCLUSION

Article 235 of Law 20 of 2025 recognises electronic evidence while leaving technical authentication questions to scientifically informed procedural practice. A defensible reform would clarify collection, provenance, lawful acquisition, independent testing, disclosure, expert competency and recorded judicial reasons. The proposed EEAS is not binding law; a future procedural guideline must respect statutory exclusions, judicial independence, proportionality and defence rights. A hash match and AI-detector score are relevant technical observations, not substitutes for the court's legal determination.

REFERENCES

Achyarsyah, P., S. Riyadi, K. Widodo, and M. Chamim. "The Role of Digital Evidence in Criminal Law Enforcement: Challenges of Authentication and Admissibility in Court." *Research Horizon 5, no.* 6 (2025): 2987–98. https://doi.org/10.54518/rh.5.6.2025.950.

Alamsyah, P. J., K. Komarudin, D. Junaedi, R. A. A. Fikri, and F. F. Yusmar. "The Role of Electronic and Digital Forensic Evidence Methods in Modern Criminal Law Enforcement in Indonesia." *Indonesian Journal of Printing 5, no.* 3 (2026): 1028–38. https://doi.org/10.58344/jii.v5i3.7618.

Anshari, A. T. A., S. Januarita, M. Q. Dewani, J. M. Wijaya, W. S. Atmadja, and Y. P. Ginting. "The Evidentiary Power of Electronic Recordings as Testimony in the Perspective of Indonesian Criminal Law." *Sanskara Law and Human Rights* 4, no. 2 (2025): 181–91. https://doi.org/10.58812/shh.v4i02.698.

Apollo, Y. M., and K. Michael. "Beyond a Reasonable Doubt? Audiovisual Evidence, AI Manipulation, Deepfakes, and the Law." *IEEE Transactions on Technology and Society 5, no.* 2 (2024): 156–68. https://doi.org/10.1109/tts.2024.3427816.

Bawono, B. T., and H. Glaser. "The Urgency of Restorative Justice Regulation on Hate Speech." *Governance* 11, no. 2 (2024): 364. https://doi.org/10.20961/bestuur.v11i2.82508.

Begishev, I. R., and A. V. Mayorov. "Digital Transformation of Criminal Justice: Theoretical Foundations and Legal Regulation Issues." *Legal Order History Theory Practice* 48, no. 1 (2026): 67–72. https://doi.org/10.47475/2311-696x-2026-48-1-67-72.

Bhattarai, S. "Bridging the Digital Divide: The Imperative for Cyber Expertise among Nepal's Justices/Judges, Litigators, and Investigators." *KDCBAR Law Journal* 1, no. 1 (2025): 223–38. https://doi.org/10.3126/kdcbar.v1i1.86735.

Billah, R. S., and H. Saragih. "Challenges of Cybercrime Law Enforcement for Judges from the Legal Aspect of Evidence in Indonesia." *Journal of Social and Humanities Flow 5, no.* 2 (2025): 2739–47. https://doi.org/10.57250/ajsh.v5i2.1543.

Chanh, N. T. M. "Authentication of Electronic Evidence Derived from Digital Transactions and Communications." Zenodo, 2025. https://doi.org/10.5281/zenodo.17926440.

Chauhan, Kislay. "Digital Evidence and Emerging Technologies." *Indian Journal of Law* 4, no. 2 (2026): 17–22. https://doi.org/10.36676/ijl.v4.i2.188.

Delfino, Rebecca. "Deepfakes on Trial 2.0: A Revised Proposal for a New Federal Rule of Evidence to Mitigate Deepfake Deceptions in Court." *Loyola Law School, Los Angeles Legal Studies Research Paper No. 2025-10, February* 15, 2025. https://doi.org/10.13140/RG.2.2.12632.61447. Available at SSRN: https://ssrn.com/abstract=5188767.

Dewi, M. N. S., and M. Muslem. "The Validity of Artificial Intelligence Evidence in the Judicial System: A Juridical Analysis." *Journal of Sharia Jurisprudence of Islamic Economic Legislation* 17, no. 2 (2025): 320–34. https://doi.org/10.32505/jurisprudensi.v17i2.11022.

Dickson, P., M. Manuputty, and Y. P. Ginting. "The Evidentiary Power of Digital Conversations as Unregulated Evidence in the Criminal Code." *Journal of Law and Human Rights Sciences* 4, no. 3 (2025): 521–35. https://doi.org/10.58812/jhhws.v4i03.2727.

Dissanayake, Y. B. "Reforming Sri Lankan Law to Address Deep Fakes: Ensuring Admissibility of Contemporary Recordings in Evidence." *KDU Journal of Multidisciplinary Studies* 7, no. 2 (2025): 1–9. https://doi.org/10.4038/kjms.v7i2.201.

El-Gayar, M. M., M. Abouhawwash, S. Askar, and S. Sweidan. "A novel approach for detecting deep fake videos using graph neural networks." *Journal of Big Data* 11, no. 1 (2024). https://doi.org/10.1186/s40537-024-00884-y.

Fahlani, S. A., E. T. Rahman, M. A. Ilmy, and A. Mursal. "The Position and Evidentiary Strength of Deepfakes in the Trial Process." Shilap Journal of Lepidopterology, 2026. https://doi.org/10.31602/al-adl.v18i1.18914.

Fernando, D., D. D. Heniarti, and C. A. F. Zakaria. "Transformation of Electronic Evidence Using Digital Forensics in the Reform of Criminal Procedure Law." *Journal of Justiciabelen (JJ) 5, no.* 1 (2025): 60. https://doi.org/10.35194/jj.v5i01.5506.

Flora, H. S., M. T. H. Thuong, and R. D. Erawati. "The Orientation and Implications of New Criminal Code: An Analysis of Lawrence Friedman's Legal System." *IUS Journal of Law and Justice Studies* 11, no. 1 (2023): 113–25. https://doi.org/10.29303/ius.v11i1.1169.

Fuller, Lon L. The Morality of Law. Revised edition. New Haven: Yale University Press, 1969, 33–38.

Garrett, B.L., and C. Rudin. "Interpretable Algorithmic Forensics." *Proceedings of the National Academy of Sciences* 120, no. 41 (2023). https://doi.org/10.1073/pnas.2301842120.

Gerry, M., and R. E. Rizkiana. "The Optimization Strategy of E-Courts Organizing Quality in Indonesia." *UNTAG Law Review* 7, no. 1 (2023): 11. https://doi.org/10.56444/ulrev.v7i1.3874.

Ginting, Y. P., A. C. G. Tumbelaka, B. D. Paulin, B. Natanael, E. J. Tiasono, E. Hamonangan, M. Cahaya, M. Samy, M. C. Darmawan, and Z. N. Firliyani. "The Application of E-Litigation in Civil Cases as a Form of Civil Procedural *Law Reform* in Indonesia." *Journal of Law and Human Rights Wara Ciencias* 4, no. 3 (2025): 491–502. https://doi.org/10.58812/jhhws.v4i03.2723.

Grossman, M., and P. Grimm. "Judicial Approaches to Acknowledged and Unacknowledged AI-Generated Evidence." *Science and Technology Law Review* 26, no. 2 (2025). https://doi.org/10.52214/stlr.v26i2.13890.

Handayani, D. A. "The Effectiveness of E-Court Civil Cases during the Pandemic and Post-COVID-19 Pandemic in Makassar." *Legal Issues* 52, no. 2 (2023): 119–30. https://doi.org/10.14710/mmh.52.2.2023.119-130.

Hardyansah, R., and R. Saputra. "Convergence and Divergence: Strategies for Proving Digital Evidence in Common Law and Indonesian Law Systems." *Journal of Sovereign Law* 9, no. 1 (2026): 74. https://doi.org/10.30659/jdh.v9i1.51432.

Humulhaer, S. "The Harmonization of Law Enforcement in the Eradication of Criminal Acts of Corruption." *Journal of Law Reform* 10, no. 2 (2023): 203. https://doi.org/10.26532/jph.v10i2.31329.

Istiqomah, W., M. Sood, and Muh. Risnain. "Juridical Analysis of Electronic-Based Use Rights Certificates: Study at Mataram City National Land Agency Office, Indonesia." *Path of Science* 10, no. 1 (2024): 8034–45. https://doi.org/10.22178/pos.100-36.

Kerdvibulvech, C. "Big Data and AI-Driven Evidence Analysis: A Global Perspective on Citation Trends, Accessibility, and Future Research in Legal Applications." *Journal of Big Data* 11, no. 1 (2024). https://doi.org/10.1186/s40537-024-01046-w.

Khan, M. I., and I. Ahmed. "A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime and Digital Evidence." *5, no.* 2 (2024): 1–29. https://doi.org/10.63125/96ex9767.

Kothari, S. P., and S. Tibrewala. "AI's Trojan Horse: The Deepfake Conundrum under the Criminal Justice System." *GLS KALP: Journal of Multidisciplinary Studies* 4, no. 3 (2024): 45–53. https://doi.org/10.69974/mtzxrc12.

Kusnadi, K. D., and S. A. Wiraguna. "Legal Development for Electronic Evidence in Civil Litigation: Challenges and Future Expectations." *SENTRI Journal of*

Scientific Research 4, no. 12 (2025): 3866–70. https://doi.org/10.55681/sentri.v4i12.5102.

Martinez, A. L. "Jurisvision of Deepfake Financial Documents: Semiotic Disruption and Remediation in Post-Textual Evidence." *International Journal for the Semiotics of Law, June* 3, 2026. https://doi.org/10.1007/s11196-026-10514-w.

Monique, C., Y. Yuliati, and F. Sulistio. "Exploring the Role of Digital Forensics in Identifying Cyber Crime in Indonesia's Criminal Procedure Law." *Pena Justisia: Media Communication and Legal Studies* 23, no. 2 (2024): 825. https://doi.org/10.31941/pj.v23i2.4068.

Nath, S. G., K. Summers, J. Baek, and G. Ahn. "Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics." 2024, 11–20. https://doi.org/10.1109/tps-isa62245.2024.00012.

Nurkholisah, S., D. Rismana, A. E. Nugroho, A. Munjiyah, and Q. Ayunisa. "Deepfakes as a New Form of Cybercrime: Challenges of Criminalization in Indonesian Criminal Law." *Journal of USM Law Review* 8, no. 3 (2025): 2421–45. https://doi.org/10.26623/julr.v8i3.13060.

Ojanen, A. "Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act." *European Journal of Risk Regulation* 16, no. 4 (2025): 1440–55. https://doi.org/10.1017/err.2025.10024.

Pergolizzi, J. V., and J. A. LeQuang. "Black Robes and White Coats: Daubert Standard and Medical and Legal Considerations for Medical Expert Witnesses." *Cureus* 16, no. 9 (2024). https://doi.org/10.7759/cureus.69346.

Peruzzi, E., and G. Cesar. "The Gatekeeper's Dilemma: Expert Testimony, Scientific Knowledge and Judicial Reasoning." *SSRN Electronic Journal* (2024). https://doi.org/10.2139/ssrn.4763570.

Pestana, G., W. Antunes, and J. Carvalho. "Digital Chain of Custody Operational Framework." 2023, 417–22. https://doi.org/10.1109/techdefense59795.2023.10380890.

Purnomo, H. B., R. H. S. Akili, and R. W. Amu. "Analysis of the Effectiveness of Electronic Criminal Trials." *Mutiara Journal of Research and Scientific Works* 2, no. 3 (2024): 69–79. https://doi.org/10.59059/mutiara.v2i3.1237.

Rifqi, P. A., Samsidar, and H. C. J. Salmon. "Screenshots, Chats, and Voice Notes: Rethinking Evidence in Criminal Trials." *Journal of Criminal Justice* 2, no. 6 (2026): 43–51. https://doi.org/10.62872/0hb7ee97.

Rustamaji, M., S.M. Sitompul, and A.R. Khoiruddin. "Reforming the Role of Judges in Assessing Evidence Authenticity and Legality: A Comparative Study Using the Exclusionary Rule Approach." *Media Iuris* 9, no. 1 (2026): 153–180. https://doi.org/10.20473/mi.v9i1.77218.

Saputra, A. D., H. T. Irwanto, and N. Nurisnah. "Measuring Judicial Accountability in the Algorithmic Era: Juridical Implications of Using Judicial Assistants and Black Box Risks in Constructing Judgment Arguments." *SIGn Journal of Law* 7, no. 2 (2025): 958–73. https://doi.org/10.37276/sjh.v7i2.570.

Setiadi, S. "Optimization of Humanist Law Enforcement in Order to Realize the Paradigm of Civilian Police." *Unnes Law Journal* 9, no. 1 (2023). https://doi.org/10.15294/ulj.v9i1.66846.